Hacking y Pentesting con Python

Módulo 7: Rutinas de Red Teaming con Python.

eip ESCUELA INTERNACIONAL POSGRADOS

Rutinas de Red Teaming con Python.

ACTIVIDAD MODULO 7

Objetivos

- Familiarizarse con las técnicas y herramientas básicas utilizadas en procesos de Red Teaming.
- Crear rutinas que faciliten el registro de las actividades que realiza un usuario en su sistema.
- Aprender a utilizar las librerías disponibles en Python para la creación de KeyLoggers.

Contenido correspondiente a módulo 7:

1. Introducción al uso de TOR y cómo implementar scripts en Python que permitan controlar instancias de TOR.
2. Uso de librerías en Linux y Windows para el registro de actividades.
3. Gestión y control de KeyLoggers en el entorno de red.

Actividad relacionada con el módulo 7:

1. Desplegar uno de los scripts de “KeyLogger” en su correspondiente sistema Linux o Windows. El alumno puede elegir el script y sistema operativo que prefiera.
2. Crear un servidor TCP en Python que permita obtener los eventos del teclado producidos por el script de Keylogger.

3. El servidor TCP creado en el paso anterior se encargará de guardar ficheros de texto con las pulsaciones del teclado en la máquina víctima. Cuando se haya alcanzado un total de 1000 caracteres, el script debe crear un nuevo fichero y limpiar el buffer donde se guardan los caracteres para poder rellenarlo otra vez con los siguientes 1000. No se deben sobre escribir los ficheros.
4. Paralelamente, se debe crear una rutina simple en Python que permita analizar los ficheros que va produciendo el servidor TCP. Se debe leer el directorio donde los ficheros se encuentran almacenados, leerlos uno a uno y encontrar patrones interesantes, tales como las palabras “password”, “usuario”, “http://”, “ssh ” y opcionalmente direcciones IP y de correo electrónico.